PURPOSE

Pursuant to MCL 15.654, Michigan Department of Health and Human Services is considered a Noncriminal Justice Agency (NCJA) and is an Authorized Recipient (AR), wherein certain Authorized Personnel can request and receive fingerprint-based Criminal History Record Information (CHRI) checks. Authorization for ARs to receive CHRI is for the purpose of employment determinations. Therefore, Michigan Department of Health and Human Services is to ensure compliance with applicable state and federal laws, applicable rules and regulations, and the most current version of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, in addition to Michigan Department of Health and Human Services policies, procedures, and processes. This Information Security Policy provides the appropriate access, maintenance, security, confidentiality, dissemination, integrity, and audit requirements of CHRI in all its forms, whether at rest or in transit.

The most stringent requirement shall prevail if conflict(s) is/are found between agency policies, state or federal laws, with the most current version of the FBI CJIS Security Policy, and corresponding rules or regulations.

DEFINITIONS

Authorized Recipients

An authorized recipient can be any of the following:

- A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order.
- A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes.
- A government agency authorized by federal statute, executive order, or state statute approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Authorized User/Personnel

An individual, or group of individuals, appropriately vetted through a national fingerprint-based background check, where required, and granted access to CJI data, wherein access is only for the purpose

of evaluating an individual's qualifications for employment or assignment.

USER AGREEMENT

Michigan Department of Health and Human Services shall complete and maintain a Noncriminal Justice Agency User Agreement for Release of Criminal History Record Information (RI-087) provided by the Michigan State Police (MSP). Agreements are in place to provide for data ownership, individual roles, responsibilities, etc. The Michigan Department of Health and Human Services shall complete and return a new user agreement in the event they have a legal name change, they move to a new physical address, or they wish to add or remove fingerprint reason codes. The most current copy of this user agreement will be maintained on file at the agency indefinitely.

LOCAL AGENCY SECURITY OFFICER (LASO)

The Office of Human Resources director will designate a LASO by means of completing and returning to the MSP, Security & Access Section (SAS), a Noncriminal Justice Agency Local Agency Security Officer Appointment (CJIS-015). An individual designated as the LASO is:

- Authorized user/personnel.
- An individual that has completed a fingerprint-based background check, where required, and found appropriate to have access to CHRI.
- If a school, the LASO is an employee directly involved in evaluating an individual's qualifications for employment or assignment.

A LASO is responsible for the following:

- Identifying who is using or accessing CHRI and/or systems with access to CHRI.
- Identifying and documenting any equipment connected to the state system.
- Ensuring personnel security screening procedures are being followed as stated in this policy.

- Confirming the approved and appropriate security measures are in place and working as expected.
- Supporting policy compliance and ensuring the MSP Information Security Officer (ISO) is promptly informed of security incidents.

When changes in the LASO appointment occur, Michigan Department of Health and Human Services shall complete and return a new LASO appointment form. The most current copy of the LASO appointment form will be kept on file indefinitely by the agency (CJIS-015).

All MSP fingerprint account changes are to be made by the LASO.

PERSONNEL SECURITY

PERSONNEL TERMINATION

The LASO or authorized designee shall terminate access to CHRI immediately, which is within 24 hours of a notification that an individual's termination of employment has occurred.

- The outgoing LASO's direct supervisor will notify the Office of Human Resources immediately upon termination via e-mail.
- The outgoing LASO will provide all access cards and keys to access physical CHRI media immediately upon termination. Keys must be handed over in person and cannot be left unattended.
- CHRISS access will be revoked immediately upon separation. Outgoing LASO supervisor will appoint a new LASO by submitting a CJIS-015 within 24 hours of separation.

PERSONNEL TRANSFER

Individuals with access to CHRI, and where the individual has been reassigned or transferred, shall have his or her access reviewed by the LASO or authorized designee to ensure access is still appropriate. If access is determined to be suspended, the individual shall be restricted from access to CHRI within the immediate 24 hours of transfer or reassignment and the following steps shall be taken by Michigan Department of Health and Human Services immediately:

- CHRISS Administrator will review CHRI access.
- CHRISS administrator will be notified via e-mail within 24 hours of LASO transfer by LASO's direct supervisor.
- CHRISS Administrator will receive communication from transferring LASO's supervisor that outlines how their position duties have changed. CHRISS Administrator will then determine whether LASO still requires access to CHRI.
- If the CHRISS Administrator determines that the transferring LASO should no longer have access to CHRI, the Administrator will then revoke their access via CHRISS within 24 hours of transfer.

SANCTIONS

Persons found noncompliant with state or federal laws, current FBI CJIS Security Policy, rules or regulations, including Michigan Department of Health and Human Services Information Security Policy, will be formally disciplined. Discipline can be, but not limited to, counseling, the reassignment of CHRI responsibilities, dismissal, or prosecution. Discipline will be based on the severity of the infraction and at the discretion of Michigan Department of Health and Human Services.

IV-D staff with access to CHRI and/or CHRISS are liable for the unauthorized disclosure of CHRI. This offense is punishable by a fine of not more than $10,000. Additionally, at a IV-D office's discretion, IV-D staff may be subject to counseling, the reassignment of CHRI responsibilities, dismissal, or prosecution for unauthorized disclosures of CHRI.

MEDIA PROTECTION

CHRI media is to be protected and secured at all times. The following is established and is to be implemented to ensure the appropriate security, handling, transporting, and storing of CHRI media in all its forms.

MEDIA STORAGE and ACCESS

Digital and physical CHRI media shall be securely stored within physically secured locations or controlled areas, and within the agency's facility unless otherwise permitted. Access to such media is restricted to authorized personnel only and secured at all times when not in use or under the supervision of an authorized individual.

Physical CHRI media:

- Is to be stored within individual records when feasible or by itself when necessary.
- Is to be maintained within a lockable filling cabinet, drawer, closet, office, safe, vault, etc.

Digital CHRI media:

- Is to be secured through encryption as specified in the most current FBI CJIS Security Policy.
- Unless encrypted, digital storage media devices (such as discs, CDs, SDs, thumb drives, DVDs, etc.) are to be maintained within a lockable filling cabinet, drawer, closet, office, safe, vault, etc.

MEDIA TRANSPORT (DIGITAL AND/OR PHYSICAL)

Should the need arise to move CHRI media outside of the secured location or controlled area, the Michigan Department of Health and Human Services shall establish and implement appropriate security controls to prevent compromise of the data while transporting. The transport of CHRI media will be conducted by authorized personnel.

CHRI media includes:

- Physical CHRI media such as paper/hard copies.
- Digital CHRI media such as laptops; computer hard drives; and any removable, transportable digital memory media, such as

magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card(s).

- Agency LASO will handle and transport physical CHRI.
- Transport will occur for employment determination; approved by LASO, CHRISS Administrator, and direct supervisors of LASO and CHRISS Administrator.
- CHRI will be printed from a secure printer and transported via locked briefcase to the destination.
- CHRI media is to always remain in the possession of agency LASO for the duration of the transport.

DISPOSAL OF PHYSICAL MEDIA

Once physical CHRI media (paper copies) is determined no longer needed by the agency, media shall be destroyed and disposed of according to the FBI CJIS Security Policy. Formal procedures for the secure disposal or destruction of physical media:

- MDHHS will formally document all instances of physical CHRI destruction. Documentation will be signed and dated by all authorized parties witnessing the destruction of CHRI.
- Destruction of physical CHRI media will be witnessed by authorized LASO and CHRISS administrator. At least 2 authorized personnel will be required to witness and document the destruction of CHRI.
- MDHHS will carry out the destruction of physical CHRI media via crosscut shredding.

PHYSICAL PROTECTION

Michigan Department of Health and Human Services shall document and implement a physical protection policy and procedures to ensure CHRI and information system hardware, software, and media are physically protected through access control measures.

PHYSICALLY SECURE LOCATION

Michigan Department of Health and Human Services will ensure both sufficient physical and personnel security controls exist for the protection of CHRI and associated information systems. A physically secure location is a facility, an area, a room, or a group of rooms within a facility. Michigan Department of Health and Human Services will:

- Prominently post the perimeter of the physically secured location and keep separate from non-secure locations by physical controls.
- Keep a current list of personnel with authorized access to the physically secure location or use a method of credentials to keep track of authorized personnel.
- Ensure all physical areas where CHRI or information systems are stored and/or used for processing shall be controlled. Individuals requiring access to such locations will be verified before granting access. Physical access to information system distribution and transmission lines within the physically secure location will be controlled and safeguarded.
- Position information system devices that display CHRI in such a way as to prevent unauthorized individuals from accessing and viewing CHRI.
- Ensure methods are in place to monitor, detect, and respond to information system incidents for individuals attaining physical access to secured areas.
- Validate all visitors before admittance to the physically secure locations, and visitors will be escorted and monitored at all times.
- Authorize and control information system-related items entering and exiting the physically secure location.

CONTROLLED AREA

If an agency cannot meet all of the controls required for establishing a physically secure location but has an operational need to access or store CHRI, the agency shall designate an area,

a room, or a storage container, as a controlled area for the purpose of day-to-day CHRI access or storage. At a minimum:

- Access is limited to controlled area during CHRI processing times and to authorized personnel, approved by the agency to access or view CHRI.
- CHRI will be locked and secured to prevent unauthorized access when unattended.
- Information system devices and documents containing CHRI will be positioned in such a way as to prevent an unauthorized individual from access or view.
- Encryption requirements will be implemented for digital storage (i.e. data “at rest”) of CHRI.

INCIDENT RESPONSE

Michigan Department of Health and Human Services shall establish operational incident handling procedures for instances of an information security breach. Information security incidents are major incidents that significantly endanger the security or integrity of CHRI. The agency will identify responsibilities for information security incidents and include how and who to report such incidents to. The agency will ensure appropriate security incident capabilities exist, and should incorporate the lessons learned from ongoing incident handling activities. The agency will ensure procedures exist and are implemented for a follow-up action of a security breach and for the collection of evidence in cases of legal action. All individuals with direct or indirect access to CHRI shall be trained on how to handle an information security incident, and such training is to be included within the agency’s Security Awareness Training. (See section on Security Awareness Training at the end of this document.) Procedures shall be in place to track and document information security incidents, whether physical or digital, on an ongoing basis. When an incident has been determined a breach involving CHRI, the agency will report the security breach to the MSP ISO by use of the “Information Security Officer (ISO) Computer Security Incident Response Capability Reporting” form (CJIS-016).

1. IV-D staff will immediately report potential or confirmed compromises of CHRI by completing the Security Incident Report (DHS-882) and sending it to their supervisor. Supervisors will follow the directions on the DHS-882 for reporting the incident and sending the form to OCS. The OCS security analyst will review the incident, and MDHHS HR personnel (LASO) will report potential or confirmed compromises of CHRI to the MSP Information Security Officer by completing the CJIS-016 form.

2. Handling Capabilities implemented by the agency:

Capabilities shall be handled according to the following description:	Physical – Hard Copy CHRI	Digital – Digitally Accessed/Saved CHRI
1. Preparation	The CHRI container will be locked at all times in the business office which will be locked when office staff is not present. (The Grand Tower utilizes video surveillance to monitor the perimeter and points of entry at the ground floor. Video surveillance provided by DTMB central control.)	Firewalls, virus protection, and malware/spyware protection will be maintained.
2. Detection	Physical intrusions to the building will be monitored by means of: The Grand Tower is monitored using video surveillance, card readers at entry points, and door alarms at entry points. All surveillance and monitoring tools are provided by DTMB central control. In addition, the building is also monitored by DTMB personnel outside of business hours and on holidays.	Electronic intrusions will be monitored by the virus and malware/spyware detection.
3. Analysis	The LASO will work with police authorities to determine how the incident occurred and what data were affected.	IT department will determine what systems or data were compromised and affected.
4. Containment	The LASO will lock uncompromised CHRI in a secure container or transport CHRI to secure area.	The IT department will stop the spread of any intrusion and prevent further damage.
5. Eradication	The LASO will work with law enforcement (Michigan State Police)	The IT department will remove the intrusion before

Capabilities shall be handled according to the following description:	Physical – Hard Copy CHRI	Digital – Digitally Accessed/Saved CHRI
	to remove any threats that compromise CHRI data.	restoring the system. All steps necessary to prevent recurrence will be taken before restoring the system.
6. Recovery	The law enforcement agency (Michigan State Police) in charge will handle and oversee recovery of stolen CHRI media. The LASO may contact MSP for assistant in re-fingerprinting if necessary.	The IT department will restore the agency information system and media to a safe environment.

When investigating an incident, the case will be sent to MDHHS Labor Relations and MDHHS Security and Compliance to begin investigation protocols. Either entity will notify local law enforcement in the county or city of the offense. MDHHS operates in 83 counties and jurisdiction would be determined on a case-by-case basis.

3. Reporting an Incident

FOC, PA, AG and SCAO Offices

The IV-D office director or his/her designee will immediately report potential or confirmed compromises of CHRI to the MSP Information Security Officer by completing the MSP form Information Security Officer (ISO) Security Incident Report (CJIS-016). Instructions for submitting

OCS, DTMB, and MiSDU State and Contracted IV-D Staff

IV-D staff will immediately report potential or confirmed compromises of CHRI by completing the Security Incident Report (DHS-882) and sending it to their supervisor. Supervisors will follow the directions on the DHS-882 for reporting the incident and sending the form to OCS. The OCS security analyst will review the incident, and MDHHS HR personnel will report potential or confirmed compromises of CHRI to the MSP Information Security Officer by completing the CJIS-016 form.

4. The MDHHS Agency LASO will When permitted by law, and Michigan Department of Health and Human Services releases a CHRI response to another authorized recipient pursuant to authorized sharing provisions, a log of such release(s) shall be established, implemented, and kept current. The log will be maintained indefinitely and be made available upon request to a MSP representative for audit purposes. Fields required for the log are:

- The date the record was shared.
- Record disseminated.
- Requesting agency.
- Requestor's name.
- Method of sharing; either by U.S. Mail, landline fax, or within the Criminal History Record Internet Subscription Service (CHRISS). (No emailing unless encrypted).
- Agency personnel that shared the CHRI.

SECURITY AWARENESS TRAINING

Michigan Department of Health and Human Services will establish, implement, and administer basic Security Awareness Training (SAT) that meets the minimum standards provided within the most current version of the FBI CJIS Security Policy. The LASO will, every two years and starting from date of adopting agency SAT, review the FBI CJIS Security Policy to ensure agency implemented SAT meets the most current requirement(s). All individuals having access to CHRI, whether digital or physical, shall complete SAT provided by the agency within six (6) months of assignment and every two (2) years thereafter. The agency will also include any or all Information Technology (IT) personnel having access to digital systems used to process CHRI. The agency will document and keep current completed SAT records, past and current.